AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) [[-]] A method ~~Method making it possible~~ to detect and/or to avoid the modification of software embedded in a programmable memory within a system comprising a hard kernel containing hardware security functions suitable for verifying the integrity of a soft kernel comprising a programmable memory, the system comprising a local data interface, ~~characterized in that it comprises~~ comprising ~~at least~~ the following steps:

~~A1 the signal received on the local data interface is not valid, place~~ placing the system in a disabled state if the signal received on the local data interface is not valid;

~~B1 the signal received on the local data interface is a disconnection signal, or there is no signal, instigate~~ instigating a secure startup procedure, with execution of the control functions if the signal received on the local data interface is a disconnection signal, or there is no signal;

~~Autotest~~ auto testing of the hard kernel wherein:

~~• If the auto test is OK, then test the integrity of the reprogrammable memory,~~

~~o If this integrity is OK, then activate the system for normal operation~~

~~o If this integrity is KO, then place the system in a disabled state~~

~~• If the auto test is KO, then place the system in a disabled state,~~

~~C1 the received signal is a valid startup signal,~~

~~• If the system is in a development mode, render it enabled,~~

~~• If the system is in an enabled utilization mode and if the signal is a test signal, then deactivate at least one of the essential functions of enabled operation.~~

if the auto test is OK, then test the integrity of the reprogrammable memory;

if this integrity is OK, then activate the system for normal operation;

if this integrity is KO, then place the system in a disabled state;

if the auto test is KO, then place the system in a disabled state;

wherein if the received signal is a valid startup signal;

if the system is in a development mode, render it enabled;

if the system is in an enabled utilization mode and if the signal is a test signal, then deactivate at least one of the essential functions of enabled operation.

2. (Currently Amended) [[-]] A method ~~Method making it possible~~ to detect and/or to avoid illicit modifications of manufacturer software within a GSM-type system, comprising a hard kernel and a soft kernel, a local data interface, comprising at least the following steps:

~~A2 the signal received on the local data interface of the terminal is not valid, place~~ placing the GSM terminal in a disabled state, if the signal received on the local data interface of the terminal is not valid;

~~B2 the signal received on the local data interface is a disconnection signal, or there is no signal, instigate~~ instigating a secure startup procedure, with execution of the control functions if the signal received on the local data interface is a disconnection signal, or there is no signal:

~~Autotest~~ auto testing of the hard kernel wherein:

~~• If the auto test is OK, then test the integrity of the soft kernel~~

~~o If this integrity is OK, then activate the terminal for normal operation,~~

~~o If the integrity is KO, then place the terminal in a disabled state,~~

~~• If the auto test is KO, then place the GSM terminal in a disabled state.~~

~~C2 the received signal is a valid startup signal:~~

~~• If the fuse is not blown, render the GSM terminal enabled,~~

~~• If the fuse is blown, render the terminal not totally enabled, by deactivating at least one of the enabled functions of the terminal:~~

~~o If the signal is a signal of JTAG test type, continue the test procedure,~~

~~o If the signal is a test signal, start up in nonsecure mode and continue the test procedure.~~

if the auto test is OK, then test the integrity of the soft kernel;

if this integrity is OK, then activate the terminal for normal operation;

if the integrity is KO, then place the terminal in a disabled state;

if the auto test is KO, then place the GSM terminal in a disabled state;

wherein if the received signal is a valid startup signal;

if the fuse is not blown, render the GSM terminal enabled;

if the fuse is blown, render the terminal not totally enabled, by deactivating at least one of the enabled functions of the terminal;

if the signal is a signal of JTAG test type, continue the test procedure,

if the signal is a test signal, start up in nonsecure mode and continue the test procedure.

3. (Currently Amended) [[-]] The method ~~Method~~ according to ~~one of Claims 1 and 2~~ claim 1, ~~characterized in that~~ wherein the exchange of the data between the hard kernel and the soft kernel is performed by using an algorithm based on the principle of non-replay and of nonpredictability of the transmitted data.

4. (Currently Amended) [[-]] The system ~~System~~ making it possible to detect and/or to avoid the modification of software embedded in a programmable memory comprising a hard kernel containing hardware security functions and a soft kernel comprising a programmable memory, a local data interface able to receive signals, characterized in that it comprises means suitable to:

- ~~place the system in a disabled state when the signal received on the local data interface is not valid,~~
- ~~for a disconnection signal received or an absence of signal on the local data interface, instigate a secure startup procedure, with execution of control functions:~~

~~Autotest of the hard kernel:~~

- ~~If the auto test is OK, then test the integrity of the programmable memory,~~
  - ~~If this integrity is OK, then activate the system for normal operation~~
  - ~~If this integrity is KO, then place the system in a disabled state~~
- ~~If the auto test is KO, then place the system in a disabled state,~~
- ~~For a received signal is a valid startup signal,~~
- ~~If the system is in a development mode, render it enabled,~~
- ~~If the system is in an enabled utilization mode, and if the signal is a test signal then deactivate at least one of the essential functions of enabled operation on startup.~~

placing the system in a disabled state when the signal received on the local data interface is not valid;

for a disconnection signal received or an absence of signal on the local data interface, instigating a secure startup procedure, with execution of control functions:

auto testing of the hard kernel wherein:

if the auto test is OK, then test the integrity of the programmable memory;

if this integrity is OK, then activate the system for normal operation;

if this integrity is KO, then place the system in a disabled state;

if the auto test is KO, then place the system in a disabled state;

for a received signal is a valid startup signal;

if the system is in a development mode, render it enabled;

if the system is in an enabled utilization mode, and if the signal is a test signal then deactivate at least one of the essential functions of enabled operation on startup.

5. (Currently Amended) [[-]] The system ~~System~~ according to Claim 4, characterized in that it comprises means of securing the data exchanges between the hard kernel and the soft kernel.

6. (Currently Amended) [[-]] The system ~~System~~ according to Claim 4, characterized in that the system is a GSM terminal.

7. (Currently Amended) [[-]] The system ~~System~~ according to Claim 4, characterized in that the system is a micro-computer.

8. (Currently Amended) [[-]] The system ~~System~~ according to Claim 4, characterized in that the system is an MP3-type reader containing a reprogrammable memory.

9. (New) The method according to claim 2, wherein the exchange of the data between the hard kernel and the soft kernel is performed by using an algorithm based on the principle of non-replay and of nonpredictability of the transmitted data.